Inspectie Veiligheid en Justitie
Ministerie van Veiligheid en Justitie

Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum

Thematisch inspectieonderzoek

Inhoudsopgave

Voorwoord

Van oudsher worden de termen 'rampen' en 'crises' geassocieerd met fysieke veiligheid. De afgelopen jaren hebben zich echter nieuwe vormen van risico's, dreigingen en crises voorgedaan die een andere aanpak en strategie vragen dan de klassieke rampenbestrijding en waar de Inspectie Veiligheid en Justitie haar toezicht dus ook op moet richten.

Cyberdreiging is een van die nieuwere risico's die prominent op de agenda staat. Voor het ministerie van Veiligheid en Justitie is het weerbaar maken van Nederland op het cyberdomein een speerpunt. Het Nationaal Cyber Security Centrum van de Nationaal Coördinator Terrorismebestrijding en Veiligheid is de organisatie die hier invulling aan geeft.

De Inspectie Veiligheid en Justitie levert, vanuit haar onafhankelijke rol, hier een bijdrage aan. Op verzoek van het Nationaal Cyber Security Centrum heeft de Inspectie een onderzoek verricht naar een van zijn producten, namelijk de beveiligingsadviezen. De Inspectie heeft dit onderzoek niet verricht om te beoordelen of aangesloten organisaties de beveiligingsadviezen opvolgen. In een internationaal speelveld met publieke en private organisaties, past dit niet. In dit onderzoek neemt de Inspectie haar signalerende rol aan en maakt zij inzichtelijk hoe een beveiligingsadvies tot stand komt en op welke wijze organisaties daar mee omgaan. Daarbij wijst de Inspectie op mogelijke risico's en geeft zij mogelijk verbeterpunten aan.

J.G. Bos
Hoofd van de Inspectie Veiligheid en Justitie

Samenvatting

Inleiding

De Inspectie Veiligheid en Justitie heeft op verzoek van het Nationaal Cyber Security Centrum (NCSC) onderzoek verricht naar de wijze waarop publieke en private organisaties omgaan met de adviezen die aan hen worden verstrekt. Het NCSC is de organisatie die zich namens de overheid inzet voor een veilig en open cyberdomein. Het doet dit onder andere door kennis en expertise vanuit verschillende sectoren te bundelen en te delen met andere partijen. Het NCSC biedt een aantal producten en diensten aan zijn partners aan, om hun digitale weerbaarheid te vergroten. Partners zijn overheidsorganisaties en private organisaties die zijn aangewezen als vitale infrastructuur. Een van de producten die het NCSC aanbiedt, zijn beveiligingsadviezen. Het NCSC publiceert beveiligingsadviezen wanneer de organisatie een kwetsbaarheid ontdekt in hard- of software die door (een aantal van de) partners wordt gebruikt. Beveiligingsadviezen bevatten informatie over de kwetsbaarheid, mogelijke gevolgen en bieden, indien beschikbaar, een oplossing. Vanwege het toegenomen gebruik van ICT en de toegenomen afhankelijkheid ervan, is het takenpakket van het NCSC de afgelopen jaren gegroeid. Om zijn capaciteiten zo efficiënt en effectief mogelijk in te zetten, wil de organisatie zijn producten en diensten evalueren.

Vraagstelling en onderzoek

Met dit onderzoek wil de Inspectie inzichtelijk maken op welke wijze aangesloten bedrijven en organisaties gebruik maken van de beveiligingsadviezen en hoe zij deze waarderen. Het onderzoek heeft daarmee twee onderzoeksvragen:

‘Wat doen de bij het NCSC aangesloten publieke en private partijen met de door het NCSC opgestelde beveiligingsadviezen?’

‘Welke (meer)waarde hebben de beveiligingsadviezen voor de aangesloten partijen?’

De Inspectie heeft een digitale vragenlijst uitgezet bij alle organisaties die beveiligingsadviezen van het NCSC ontvangen (de respons was 54%). Daarnaast heeft zij interviews afgenomen bij 10 organisaties, alsmede bij medewerkers van het NCSC. De Inspectie heeft haar onderzoek in de maanden oktober 2014 tot en met februari 2015 uitgevoerd. Daarbij heeft zij zich in haar onderzoek primair gericht op de beveiligingsadviezen die het NCSC heeft uitgegeven in de periode van 1 januari 2012 tot en met 1 september 2014.

Centrale conclusie

De Inspectie VenJ heeft onderzocht wat aangesloten organisaties doen met de beveiligingsadviezen van het NCSC en wat de meerwaarde ervan is voor de ontvangende partijen. Uit het onderzoek blijkt dat alle organisaties de beveiligingsadviezen van het NCSC lezen, beoordelen en indien nodig de noodzakelijke maatregelen treffen. Zij bezien hierbij of de betreffende software in gebruik is, hoe groot de kans op uitbuiting is gegeven organisatie specifieke factoren, welke gevolgen uitbuiting heeft voor de bedrijfsprocessen en hoe dringend actie nodig is.

De meeste organisaties beschouwen de beveiligingsadviezen – in de huidige vorm – als 'bruikbaar, maar niet onmisbaar'. Vaak heeft men informatie over kwetsbaarheden al via andere bronnen (zowel externe als andere informatiekanalen van het NCSC) binnengekregen en de oplossing geïmplementeerd, voordat het beveiligingsadvies is ontvangen. Voor alle partijen zit de meerwaarde van de beveiligingsadviezen niet zo zeer in de inhoud en kwaliteit, maar voornamelijk in het feit dat de adviezen afkomstig zijn van een onafhankelijke autoriteit met een gezaghebbende positie. Het NCSC kan volgens hen over de – commerciële – schotten kijken en een objectief advies leveren. Opvallend daarbij is de veronderstelling van aangesloten organisaties dat het NCSC de beveiligingsadviezen (ook) baseert op vertrouwelijke informatiebronnen waar de organisaties zelf geen toegang tot hebben. Want hoewel de aangesloten organisaties dit als belangrijke meerwaarde zien, baseert het NCSC beveiligingsadviezen in beginsel op openbare bronnen.

De Inspectie concludeert dat de beveiligingsadviezen in de huidige vorm beperkte meerwaarde hebben. De Inspectie onderschrijft de ambitie van het NCSC om haar capaciteiten zo efficiënt en effectief mogelijk in te zetten. In dat kader beveelt de Inspectie het NCSC aan om het product beveiligingsadviezen te heroverwegen. Het gaat de aangesloten organisaties uiteindelijk om de informatie over kwetsbaarheden, niet om het product of de wijze waarop ze de informatie binnen krijgen. De Inspectie gaat er vanuit dat de in dit onderzoek geconstateerde aandachtspunten hierbij betrokken worden (zie voor een volledig overzicht bijlage I).

Onderzoeksbevindingen

Doelgroep beveiligingsadviezen

- Er is sprake van een grote mate van diversiteit in de organisaties die zich hebben aangesloten bij het NCSC om beveiligingsadviezen te ontvangen. Het grootste deel bestaat uit publieke partijen met daarnaast een aantal private partijen uit vitale sectoren. De diversiteit uit zich verder in de grootte van de ICT-afdeling en de aan- dan wel afwezigheid van een afdeling die zich uitsluitend met cybersecurity bezig houdt.
- De voornaamste reden om zich aan te melden voor de beveiligingsadviezen is gelegen in de behoefte van organisaties aan zo veel mogelijk betrouwbare informatie over digitale dreigingen en kwetsbaarheden voor het eigen bedrijfsproces.

Totstandkoming en communicatie beveiligingsadviezen

- Voor het opstellen van het beveiligingsadvies maakt het NCSC hoofdzakelijk gebruik van openbare bronnen. Het NCSC wil in de beveiligingsadviezen namelijk kunnen verwijzen naar de bron, waar de kwetsbaarheid is beschreven en een oplossing wordt geboden.
- Het NCSC verifieert de verzamelde informatie en kwalificeert de kwetsbaarheden aan de hand van de kans op uitbuiting van de kwetsbaarheid en de ernst van de schade bij uitbuiting. Beide parameters worden ingeschaald als low, medium of high.

- Beveiligingsadviezen bevatten informatie over het type kwetsbaarheid en de gevolgen bij uitbuiting. Daarbij wordt verwezen naar websites waar mogelijke oplossingen zijn te vinden voor het verhelpen van de kwetsbaarheden.
- De verzending van de beveiligingsadviezen gaat per mail. Indien organisaties een actueel overzicht van in gebruik zijnde systemen hebben aangeleverd, krijgen zij de voor hen relevante beveiligingsadviezen. Daarnaast worden beveiligingsadviezen gepubliceerd op de website van het NCSC.

Gebruik van de beveiligingsadviezen
- Alle organisaties lezen (in principe) alle beveiligingsadviezen en wegen af wat het betekent voor de eigen organisatie. Organisaties bezien daarbij of ze de betreffende software gebruiken, hoe groot de kans op uitbuiting is bij hen, welke gevolgen uitbuiting heeft voor de bedrijfsprocessen en welke actie op dat moment noodzakelijk is.
- Vanwege de specifieke kenmerken van de ICT-infrastructuur kan een organisatie tot een andere inschaling van de kwetsbaarheid komen. Vaak heeft men een breder pakket aan beveiligingsmaatregelen getroffen waardoor een lek in een specifiek systeem of applicatie niet direct een grote impact hoeft te hebben. Het NCSC kan en hoeft hier niet van op de hoogte te zijn, volgens de aangesloten organisaties.
- Bij het implementeren van een oplossing, houden organisaties rekening met de gevolgen voor de bedrijfsprocessen. Oplossingen met een mogelijk hoge impact voor de stabiliteit van de bedrijfsprocessen worden eerst getest voordat ze breed worden uitgerold. In andere gevallen worden oplossingen meegenomen in reguliere patchrondes.

De waardering van de beveiligingsadviezen
- Betrokken partijen waarderen de kennis en expertise van het NCSC. Dit betreft niet alleen de beveiligingsadviezen, maar ook de andere producten die het NCSC levert (bijvoorbeeld factsheets, white papers en sectorale overlegvormen). Veel betrokkenen geven aan dat zij informatie over kwetsbaarheden vooral ook uit die andere kanalen haalt. Zij zien het NCSC als een coördinerende partij, een informatiemakelaar, die met haar eigen expertise de kennis over kwetsbaarheden kan verrijken.
- De beveiligingsadviezen van het NCSC hebben volgens respondenten een gezaghebbende status. In een internationaal speelveld met (concurrerende) private en publieke partijen, is een objectieve en onafhankelijke organisatie, die boven alle belangen staat, volgens hen belangrijk.
- In het onderzoek geven betrokkenen aan dat een belangrijke meerwaarde van het beveiligingsadvies van het NCSC het feit is dat deze, volgens hen, gebaseerd zijn op (vertrouwelijke) bronnen die voor andere organisaties niet zijn te benaderen. Dit beeld is echter niet helemaal correct. Zoals reeds is beschreven, zijn de meeste beveiligingsadviezen gebaseerd op openbare bronnen.
- Beveiligingsadviezen zijn vaak niet de eerste melding over een kwetsbaarheid die organisaties ontvangen. Dit, omdat betrokkenen vaak van dezelfde bronnen gebruik maken. De helft van de ondervraagden geeft aan de kwetsbaarheid te hebben verholpen voordat zij een advies hadden ontvangen.
- Het merendeel van de beveiligingsadviezen betreft een updatemelding van een eerder advies (2438 van de 4578 in de onderzoeksperiode). Daarnaast gaan veel beveiligingsadviezen over laag gekwalificeerde kwetsbaarheden, die doorgaans al via andere kanalen bekend zijn (bijvoorbeeld updates van Microsoft).
- De inhoud van de beveiligingsadviezen sluit niet altijd goed aan op de behoeften van organisaties. Sommige organisaties zouden graag meer technische informatie in de beveiligingsadviezen zien, anderen juist meer kwalitatieve informatie.

1 Inleiding

De laatste decennia hebben het gebruik van informatie- en communicatietechnologie (ICT) en verbondenheid via het internet een grote vlucht genomen. Naast de vele voordelen die dit biedt, brengt het ook risico's met zich mee. Vanwege de toegenomen afhankelijkheid van ICT zijn de nadelige gevolgen van misbruik namelijk ook groter geworden. Schade aan ICT, bijvoorbeeld als gevolg van cyberaanvallen, kan bestaan uit beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie.

De afgelopen jaren is helder geworden wat de potentiële impact van een cyberaanval kan zijn. In oktober 2014 werd bijvoorbeeld duidelijk hoe groot de omvang van een hack door (vermoedelijk) een Russische bende was toen het NCSC hierover publiceerde. Bij meerdere hacks werden in totaal ruim 1,2 miljard gebruikersgegevens buitgemaakt, waarbij ook 5600 Nederlandse websites waren getroffen. Jaarlijks wordt een groot aantal kwetsbaarheden ontdekt, in 2014 bijvoorbeeld al 7038.

Cybersecurity is daarom één van de belangrijkste thema's in de samenleving. Het is een speerpunt in het beleid van het ministerie van Veiligheid en Justitie. Het Nationaal Cyber Security Centrum (NCSC) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is de organisatie die zich namens de overheid inzet voor een veilig en open cyberdomein[1]. Zij doet dit onder andere door kennis en expertise vanuit verschillende sectoren te bundelen en te delen met andere partijen.

Het NCSC biedt een aantal producten en diensten aan haar partners aan, om hun digitale weerbaarheid te vergroten. Zo publiceert het NCSC beveiligingsadviezen wanneer een kwetsbaarheid is ontdekt in hard- of software die door (een aantal van de) partners wordt gebruikt. Beveiligingsadviezen bevatten informatie over de kwetsbaarheid, mogelijke gevolgen en bieden indien beschikbaar een oplossing. Daarnaast kwalificeert het NCSC de kwetsbaarheden aan de hand van de kans op uitbuiting van de kwetsbaarheid en de ernst van de schade bij uitbuiting. Beide parameters worden ingeschaald als low, medium of high.

[1] Missie Directie Cyber Security/Nationaal Cyber Security Centrum.

Vanwege het toegenomen gebruik van ICT en de toegenomen afhankelijkheid ervan, is het takenpakket van het NCSC de afgelopen jaren gegroeid. Om haar capaciteiten zo efficiënt en effectief mogelijk in te zetten, wil de organisatie haar producten en diensten evalueren. Het NCSC heeft daarom de Inspectie VenJ verzocht een onderzoek uit te voeren naar de wijze waarop organisaties omgaan met de beveiligingsadviezen die het NCSC verstrekt. Omdat cybersecurity ook voor de Inspectie een belangrijk onderwerp dat in de werkprogrammering is opgenomen, is zij ingegaan op dit verzoek.

1.1 Doel- en vraagstelling

Met dit onderzoek wil de Inspectie VenJ inzichtelijk maken op welke wijze aangesloten bedrijven en organisaties gebruik maken van de beveiligingsadviezen en hoe zij deze waarderen. Het onderzoek heeft daarmee twee onderzoeksvragen:

'Wat doen de bij het NCSC aangesloten publieke en private partijen met de door het NCSC opgestelde beveiligingsadviezen?'

'Welke (meer)waarde hebben de beveiligingsadviezen voor de aangesloten partijen?'

Om een antwoord te kunnen geven op deze vragen maakt de Inspectie het proces van de beveiligingsadviezen van begin tot eind inzichtelijk en gaat daarbij in op de volgende aspecten:

- de context van cybersecurity in Nederland, de rol van het NCSC hierin en de functie van de beveiligingsadviezen;
- de organisaties die de beveiligingsadviezen ontvangen;
- de totstandkoming van de beveiligingsadviezen: vergaren van informatie over kwetsbaarheden, het analyseren van de informatie en het opstellen van de beveiligingsadviezen;
- de wijze waarop het NCSC de beveiligingsadviezen naar de partijen communiceert;
- de wijze waarop de beveiligingsadviezen bij de partijen binnenkomen;
- de wijze waarop de partijen de beveiligingsadviezen verwerken;
- de afwegingen die partijen daarbij maken;
- de mate waarin partijen maatregelen op basis van het beveiligingsadvies treffen.

Afbakening
De Inspectie VenJ heeft haar onderzoek in de maanden oktober 2014 tot en met februari 2015 uitgevoerd. Daarbij heeft zij zich in haar onderzoek primair gericht op de beveiligingsadviezen die het NCSC heeft uitgegeven in de periode van 1 januari 2012 tot en met 1 september 2014.

1.2 Onderzoeksaanpak

In dit onderzoek hanteert de Inspectie drie verschillende onderzoeksmethoden voor het beantwoorden van de onderzoeksvragen.

Documentstudie
De Inspectie heeft verschillende documenten bestudeerd. Enerzijds betreffen dit strategie-documenten van het NCSC, anderzijds betreffen het opgevraagde overzichten van het totaal aantal uitgegeven beveiligingsadviezen in de onderzoeksperiode. In bijlage II is een overzicht opgenomen van de bestudeerde documenten.

Digitale vragenlijst
De Inspectie heeft een digitale vragenlijst uitgezet bij alle organisaties die de beveiligingsadviezen van het NCSC ontvangen. Met de vragenlijst is kwantitatief in beeld gebracht hoe organisaties omgaan met beveiligingsadviezen en welke redenen zij hiervoor hebben.

Alle 69 aangesloten organisaties zijn aangeschreven. De Inspectie heeft hiervoor gebruik gemaakt van het adressenbestand van het NCSC. Omdat een aantal adressen niet meer actueel waren, hebben uiteindelijk 63 organisaties de vragenlijst ontvangen. Hiervan hebben 34 organisaties de vragenlijst ingevuld (54 %). De Inspectie heeft daarnaast een non-responsanalyse uitgevoerd om vast te kunnen stellen of sprake was van een representatieve steekproef.
De Inspectie heeft hiervoor de respondenten die de digitale vragenlijst niet hadden ingevuld benaderd met de twee belangrijkste vragen van de vragenlijst om vast te stellen of de non-responsgroep anders antwoordde dan de responsgroep. Dit was niet het geval, waardoor de steekproef als representatief kan worden gezien.

Interviews
Voorts heeft de Inspectie verdiepende interviews gehouden bij tien organisaties die beveiligingsadviezen van het NCSC ontvangen. Gesproken is met functionarissen bij wie de adviezen binnenkomen en verantwoordelijk zijn voor de verdere afhandeling. Bij de selectie van de organisaties heeft de Inspectie VenJ met de volgende drie factoren rekening gehouden:

- Ten eerste moest de organisatie in de onderzoeksperiode minimaal één beveiligingsadvies hebben ontvangen dat in de categorie 'high high' viel, omdat hier de grootste risico's voor de samenleving zijn. Het gaat hier om kwetsbaarheden die een hoge kans op uitbuiting en een hoge kans op schade hebben.
- Ten tweede streefde de Inspectie naar een goede verdeling tussen publieke en private partijen. Gezien het beperkt aantal aangesloten private partijen, heeft de Inspectie niet gekozen voor een representatieve steekproef. In plaats daarvan heeft de Inspectie drie private partijen geïnterviewd.
- Ten derde heeft de Inspectie, bij de selectie van publieke partijen, rekening gehouden met de toezichtlast vanuit andere onderzoeken van deze Inspectie.

Tot slot heeft de Inspectie bij medewerkers zowel op operationeel, tactisch als strategisch niveau interviews afgenomen bij het NCSC.

1.3 Leeswijzer

In hoofdstuk twee geeft de Inspectie contextinformatie over het NCSC, de doelgroepen en de totstandkoming en communicatie van de beveiligingsadviezen. In hoofdstuk drie geeft de Inspectie antwoord op beide onderzoeksvragen. Hoofdstuk vier bevat een algemene conclusie waarin de Inspectie aanbevelingen doet aan het NCSC om de meerwaarde van de beveiligingsadviezen te vergroten.

2 Cybersecurity in Nederland

2.1 Het Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) is de organisatie van de overheid die bijdraagt aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein. Het centrum valt onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het ministerie van Veiligheid en Justitie. In dit hoofdstuk geeft de Inspectie een kort beeld van het NCSC, zijn totstandkoming, de taken en verantwoordelijkheden en de dienstverlening die de organisatie levert.

Van GOVCERT.NL naar Nationaal Cyber Security Centrum

In de meeste landen hebben overheden en private organisaties een zogenoemd Computer Emergency Response Teams (CERT) ingericht. In een CERT zijn deskundigen op het gebied van ICT en security werkzaam die bij cyberincidenten kunnen ingrijpen om schade te beperken dan wel te herstellen. Een CERT richt zich daarnaast op preventie.

GOVCERT.NL is sinds 2002 de CERT van de Nederlandse overheid. GOVCERT.NL viel onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De organisatie spande zich in om overheidsorganisaties en private organisaties op de hoogte te stellen van actuele kwetsbaarheden en dreigingen en bood ondersteuning in het geval van een incident.

De taken van GOVCERT.NL zijn per 1 januari 2012 opgegaan in het NCSC. Sinds de oprichting van het NCSC in 2012 heeft de organisatie taken erbij gekregen en is hij behoorlijk gegroeid in omvang. Door de schaalvergroting zijn teams binnen het NCSC meer gespecialiseerd. Medewerkers voeren meerdere taken uit, maar rouleren nu tussen verschillende teams.

De Nationale Cyber Security Strategie: beschermen van vitale belangen in het cyberdomein

Het NCSC heeft in de Nationale Cyber Security Strategie (NCSS) beschreven hoe de organisatie Nederland digitaal weerbaar wil maken. Het NCSC heeft in 2014 haar tweede strategiedocument gepubliceerd (NCSS 2.0). In deze strategie zet het NCSC uiteen welke doelen de organisatie wil bereiken en op welke manier. Het document bouwt voort op de visie:

'Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.'

Het cyberdomein is per definitie grensoverstijgend. Het NCSC bevindt zich midden in een netwerk van (internationale) publieke en private organisaties. Om hier effectief in op te treden, is positionering van de eigen organisatie van belang. De rol van de 'klassieke' sturende beleidsmaker of toezichthouder past in de visie van het NCSC in een dergelijke constellatie niet. Het NCSC ziet zichzelf daarom als een kennisautoriteit die publieke en private organisaties met elkaar verbindt teneinde relevante expertise te delen en organisaties zo weerbaar te maken tegen cyberdreigingen. Een belangrijke succesvoorwaarde die het NCSC zelf ziet, is het zijn van een betrouwbare en onafhankelijke organisatie. Dit is van belang om andere organisaties bereid te vinden informatie te delen met het NCSC.

Vanuit deze positie heeft het NCSC drie kerntaken gedefinieerd. Dat zijn achtereenvolgens:

1. Expertise opbouwen en advies geven.
2. Respons op dreigingen en incidenten.
3. Versterken van de crisisbeheersing.

Het NCSC richt zich met deze kerntaken momenteel voornamelijk op overheidsorganisaties en op private organisaties die werkzaam zijn in een vitale sector, zoals de energiesector en de financiële sector. Het NCSC richt zich met name op deze organisaties, omdat gevolgen van uitbuiting van kwetsbaarheden juist daar ernstig en zelfs ontwrichtend voor de maatschappij kunnen zijn.

Om vitale organisaties digitaal weerbaar(der) te maken, biedt het NCSC zoals gezegd meerdere diensten aan. Het NCSC stelt zich als doel om publieke en private organisaties met elkaar te verbinden om kennis en expertise op het gebied van cybersecurity te bundelen. Het NCSC heeft daarom verschillende samenwerkingsverbanden opgericht waarbinnen informatie over kwetsbaarheden en andere gerelateerde onderwerpen wordt gedeeld. Voorbeelden zijn het Nationaal Detectie Netwerk (NDN) en de sectoraal ingerichte 'Information Sharing and Analysis Centers' (ISAC's).

Het NDN is een samenwerkingsverband waarbinnen informatie over cyberdreigingen kan worden uitgewisseld. ISAC's zijn ingericht per sector. Zij hebben als doel om binnen een sector informatie op het gebied van cybersecurity in een vertrouwde setting te delen. Momenteel zijn er twaalf ISAC's operationeel in Nederland, waaronder in de energiesector en de financiële sector[2].

Naast verschillende samenwerkingsverbanden levert het NCSC ook concrete producten, zoals de beveiligingsadviezen. Daarnaast worden regelmatig white papers en factsheets gepubliceerd met daarin tips en aandachtspunten voor specifieke onderwerpen (bijvoorbeeld het beveiligingen van wifi-netwerken). De beveiligingsadviezen zijn een specifiek product waar organisaties zich voor aan moeten melden bij het NCSC.

[2] In Nederland zijn de volgende ISAC's actief: Haven-ISAC, Airport-ISAC, Financial Institutions-ISAC, Multinationals-ISAC, Telecom-ISAC, Nucleair-ISAC, Zorg-ISAC, Energy-ISAC, Water-ISAC, Managed Service Provider (MSP)-ISAC, Insurance-ISAC, Rijks-ISAC.

Beveiligingsadviezen: oplossingen aandragen bij concrete kwetsbaarheden
Beveiligingsadviezen van het NCSC zijn erop gericht om informatie over kwetsbaarheden onder de aandacht te brengen van aangesloten organisaties. Daarbij verrijkt het NCSC de informatie waarop het zich baseert en biedt, indien mogelijk, oplossingen aan. Het uiteindelijke doel is dat organisaties de kwetsbaarheden verhelpen en er zodoende minder cyberincidenten plaats vinden, of dat de impact hiervan minimaal is. Het NCSC communiceert de beveiligingsadviezen gericht aan aangesloten organisaties waar de gevonden kwetsbaarheid kan worden uitgebuit. De beveiligingsadviezen zijn daarnaast ook publiekelijk beschikbaar via de website van het NCSC.

2.2 De doelgroep van het Nationaal Cyber Security Centrum

Grote diversiteit in de groep aangesloten organisaties
Ten tijde van het onderzoek waren 65 organisaties aangemeld bij het NCSC. Het overgrote deel bestaat uit publieke partijen, een vijfde deel bestaat uit private partijen. Er blijkt een grote diversiteit in de typen organisaties te zijn. Voor dit onderzoek is gekeken naar de afdeling die de beveiligingsadviezen ontvangt. Het verschil uit zich dan in twee aspecten: de mate van security-awareness binnen de organisatie en de grootte van de ICT-afdeling.

De grotere organisaties hebben vaak een aparte cybersecurity-afdeling (met een securitymanager en security-officers) die zich uitsluitend bezig houdt met het weerbaar maken van de organisatie. Deze kunnen in omvang gelijkwaardig of groter zijn dan het NCSC. Bij de kleinere organisaties is cybersecurity vaak een taak die ‘erbij’ wordt gedaan door de ICT-afdeling of de systeembeheerder.

Redenen om aan te melden
Organisaties geven in het onderzoek verschillende redenen aan om zich aan te melden bij het NCSC voor het product beveiligingsadviezen. De belangrijkste reden is dat organisaties behoefte hebben aan zoveel mogelijk betrouwbare informatie om digitale dreigingen en kwetsbaarheden voor het eigen bedrijfsproces in beeld te krijgen. Om die reden maakt men graag gebruik van de informatie van het NCSC. Voor alle organisaties zijn de beveiligingsadviezen van het NCSC een bruikbare informatiebron in het kader van cybersecurity.

Voor veel (vooral grotere) organisaties zijn de beveiligingsadviezen een extra informatiebron (‘een extra paar ogen’). Deze organisaties hebben doorgaans zelf capaciteit om kwetsbaarheden en dreigingen te signaleren. Daarnaast hebben zij contracten afgesloten met commerciële dienstverleners die hen daarbij ondersteunen. De organisaties die internationaal opereren kunnen ten slotte ook bronnen uit andere landen aanboren. Uit het onderzoek blijkt dat 82% van de bevraagde organisaties op het gebied van cybersecurity ook gebruik maakt van (de expertise van) andere bedrijven/organisaties dan het NCSC.

Organisaties met een kleine ICT-afdeling hebben vaak minder capaciteit en middelen om zelf continu kwetsbaarheden te volgen. Voor hen heeft aanmelding voor het product beveiligings-adviezen vooral ook een financiële achtergrond. Zo stelt een respondent in dit kader:

‘Het centrale inzicht in technische kwetsbaarheden levert ons een extra bron van informatie op om potentiële beveiligingsrisico’s te beheersen en vroegtijdig gealarmeerd te worden over potentiële calamiteiten en incidenten. Het zelf inrichten hiervan is niet kostenefficiënt. Hierdoor kunnen we ons beter focussen op onze primaire taak.’

Overheidsorganisaties vinden het daarnaast over het algemeen logisch dat zij zijn aangesloten bij het NCSC. Zo stelt een respondent dat *'als onderdeel van het ministerie en met een groot deel van de gebruikers van dit ministerie een samenwerking met het NCSC onontbeerlijk is'*. Het NCSC wordt gezien als een betrouwbare overheidsondersteuner op het gebied van (informatie)beveiliging. Veelal zijn deze organisaties vanuit de tijd van GOVCERT aangesloten en is men 'meegegroeid' naar het NCSC.

Private partijen geven aan dat zij via hun deelname aan verschillende overlegplatforms, zoals de ISAC's, al samenwerken met het NCSC en vanuit die gremia kennis hebben genomen van het product beveiligingsadviezen. Zij zien aanmelding voor dit product dan als een logische vervolgstap om op verschillende niveaus informatie uit te wisselen.

2.3 Beveiligingsadviezen van het NCSC

2.3.1 Totstandkoming beveiligingsadviezen

Afdeling Monitoring en Respons verantwoordelijk voor beveiligingsadviezen
Binnen het NCSC is de afdeling Monitoring en Respons verantwoordelijk voor onder andere de beveiligingsadviezen. De waakdienst is het onderdeel van deze afdeling dat informatie verzamelt over actuele dreigingen en kwetsbaarheden. Drie medewerkers bezetten de waakdienst[3]. Tijdens de avonduren en in de nacht is één medewerker aanwezig. Het NCSC gebruikt de verzamelde informatie voor de verschillende diensten die het aanbiedt, waaronder de beveiligingsadviezen.

Het opstellen van beveiligingsadviezen gebeurt in de praktijk in drie stappen. De eerste stap betreft het raadplegen van bronnen. De tweede stap is het analyseren van de informatie om te bepalen of een beveiligingsadvies nodig is. De derde stap is het formuleren van het beveiligingsadvies.

Groot gedeelte beveiligingsadviezen is gebaseerd op openbare bronnen
Het NCSC baseert de beveiligingsadviezen in de meeste gevallen op informatie van derden. Het NCSC doet zelden actief onderzoek naar kwetsbaarheden. Informatie over kwetsbaarheden en mogelijke oplossingen zijn dus in bijna alle gevallen afkomstig van een andere partij, en is, aan de hand van andere bronnen, geverifieerd door het NCSC.

Om de benodigde informatie te vinden, maakt de waakdienst gebruik van een software-applicatie, Taranis genaamd. Taranis scant vooraf geselecteerde bronnen op ingestelde trefwoorden en ordent deze informatie voor de gebruiker. Op deze manier kunnen medewerkers veel informatiebronnen raadplegen in beperkte tijd. Taranis is aangesloten op zowel openbare als niet openbare bronnen. Openbare bronnen zijn bijvoorbeeld softwareleveranciers, fora, nieuwssites en social media. Niet openbare bronnen zijn bijvoorbeeld andere (buitenlandse) CERT's en andere vertrouwde partners in de security-gemeenschap (zoals inlichtingendiensten).

Voor het opstellen van het beveiligingsadvies maakt het NCSC echter hoofdzakelijk gebruik van openbare bronnen. De voornaamste reden hiervoor is het feit dat het NCSC in de beveiligingsadviezen wil kunnen verwijzen naar de bron. Op deze manier kan de ontvanger van het beveiligingsadvies zelf nader onderzoek plegen, indien gewenst. Bij niet openbare (gerubriceerde) bronnen is het niet mogelijk deze verdieping aan te bieden. Als het NCSC informatie van

[3] Per 1 januari 2015 heeft de waakdienst een 24/7 bezetting.

een niet-openbare bron toch wil delen, wordt het zogenoemde 'Traffic Light Protocol' (TLP) gehanteerd. Het protocol omschrijft drie mogelijke varianten van informatiedeling die corresponderen met de kleuren van een verkeerslicht: informatie mag niet gedeeld worden, informatie mag met een beperkte groep gedeeld worden of informatie mag met iedereen gedeeld worden. Indien het NCSC informatie die rood of oranje is geclassificeerd toch wil delen, vraagt de organisatie toestemming aan de bron.

Het beoordelen van signalen uit bronnen is mensenwerk

Taranis verzamelt informatie over kwetsbaarheden en dreigingen. Het systeem kan niet de inschatting maken of het bericht belangrijk is; dit is en blijft mensenwerk. Medewerkers van de waakdienst lezen daarom alle berichten die Taranis heeft gevonden en selecteren vervolgens – op basis van eigen kennis en expertise ('professional judgement') – de berichten op basis waarvan ze voornemens zijn een beveiligingsadvies op te stellen. Hier zijn geen vastgestelde criteria of checklists voor. De berichten die voor nader onderzoek worden geselecteerd, worden in het systeem aangevinkt. De andere twee medewerkers kunnen deze berichten ook zien en er beveiligingsadviezen over opstellen.

Als een medewerker besluit een beveiligingsadvies op te stellen over een gevonden kwetsbaarheid dient hij de kans op uitbuiting en de ernst van de schade bij uitbuiting te bepalen. Hiervoor heeft het NCSC een inschalingsmatrix opgesteld. Deze is te raadplegen op de website, zodat ook voor ontvangende partijen duidelijk is hoe de kwalificatie tot stand is gekomen. Medewerkers dienen voor zowel de kans op uitbuiting als de kans op schade bij uitbuiting een aantal vragen te beantwoorden op een twee- of driepuntschaal. Voorbeelden van vragen zijn of er exploitcode[4] beschikbaar is, hoe toegankelijk het systeem is en hoe complex uitbuiting is in technisch opzicht. Taranis kwalificeert vervolgens de kansen op low, medium of high. Dit resulteert in een inschaling variërend van 'low low' tot en met 'high high'. Het laatste wil zeggen dat zowel de kans op uitbuiting als de ernst van de schade bij uitbuiting hoog is.

Opstellen beveiligingsadviezen: bundelen van informatie

Na het analyseren van de informatie en het inschalen van het beveiligingsadvies, stellen medewerkers de tekst voor het advies op en gaan daarna over tot publicatie. Binnen Taranis is daarbij gewaarborgd dat wordt gewerkt conform het vier-ogen-principe: degene die een beveiligingsadvies opstelt, kan het niet publiceren. Een andere medewerker dient het eerst te controleren alvorens te publiceren.

Een beveiligingsadvies bevat algemene informatie zoals de datum van publicatie, het versienummer, de CVE-nummers[5] en dergelijke. Daarnaast bevat het beveiligingsadvies informatie over het type kwetsbaarheid en de gevolgen bij uitbuiting. Tot slot wordt in het beveiligingsadvies met een link verwezen naar websites waar mogelijke oplossingen te vinden zijn voor het verhelpen van de kwetsbaarheden of worden alternatieve oplossingen – zoals 'workarounds'– beschreven. Indien (nog) geen oplossing of work-around beschikbaar is, maar het een ernstige kwetsbaarheid betreft, publiceert het NCSC toch een beveiligingsadvies om de organisaties te alerteren.

[4] Exploitcode is software die gebruik maakt van een kwetsbaarheid.

[5] Common Vulnerabilities and Exposures (CVE) is een databank met informatie over kwetsbaarheden in computersystemen en netwerken. Iedere kwetsbaarheid krijgt een eigen nummer, zodat men op dezelfde wijze naar dezelfde kwetsbaarheid kan verwijzen. De databank wordt beheerd door het Amerikaanse bedrijf MITRE en gefinancierd door het Amerikaanse 'Department of Homeland Security'.

Alle informatie in een beveiligingsadvies is afkomstig van andere bronnen. De verrijking van het NCSC houdt in dat informatie wordt gebundeld en, indien van toepassing, wordt vertaald naar het Nederlands.

2.3.2 Communicatie van de beveiligingsadviezen

Verzending beveiligingsadviezen kan maatwerk zijn
Om op de hoogte te zijn van de hard- en software die aangesloten partijen hebben, vraagt het NCSC hen bij aanmelding om hier een overzicht van aan te leveren. Het NCSC kan de beveiligingsadviezen dan selectief versturen aan de organisaties waar ze betrekking op hebben. Het aanleveren van de informatie gebeurt met een Exceloverzicht waarop organisaties de systemen die zij in gebruik hebben kunnen aanvinken. Het overzicht wordt ook wel 'de foto' genoemd. Het overzicht wordt in Taranis geïmporteerd voor geautomatiseerde verwerking en filtering van het advies.

Het Exceloverzicht bevat een opsomming van de (meest voorkomende) hard- en software die organisaties (kunnen) gebruiken. Deze opsomming dient actueel te zijn. De mogelijkheid bestaat namelijk dat een systeem dat in gebruik is bij een organisatie, niet op het overzicht staat. Dit vormt een risico, omdat kwetsbaarheden in het betreffende systeem wel gevolgen kunnen hebben, maar niet worden gemonitord. In de praktijk zal een organisatie zelf bij het NCSC aan moeten geven dat zij systemen gebruiken die niet in het overzicht zijn opgenomen.

Verzending en publicatie verloopt via Taranis
Als een beveiligingsadvies klaar is om te verzenden, selecteert Taranis de juiste ontvangers aan de hand van de aangeleverde foto's. Als een organisatie geen foto heeft aangeleverd, ontvangt zij alle beveiligingsadviezen. De verzending gaat per e-mail naar de door de organisaties opgegeven e-mailadressen. In het geval van een 'high high' beveiligingsadvies (een hoge kans op uitbuiting en ernstige schade bij uitbuiting) belt het NCSC de contactpersonen op operationeel niveau bij de organisaties – die in de foto aangegeven hebben de betreffende systemen te gebruiken – om aandacht te vragen voor het advies.

Het NCSC kan de beveiligingsadviezen tevens in Extensible Markup Language (XML) verzenden. Dit is opmaaktaal die zowel door mensen als door machines gelezen kan worden. Een voordeel hiervan is dat de implementatie van de oplossing geautomatiseerd kan verlopen; de ontvanger hoeft zelf geen verdere actie te ondernemen omdat de computer zelf de tekst kan lezen. Uit het onderzoek blijkt dat slechts enkele partijen momenteel de beveiligingsadviezen in XML ontvangen. Dit heeft enerzijds te maken met beperkte bekendheid van deze mogelijkheid, anderzijds is het voor een aantal organisaties noodzakelijk hun systemen erop aan te passen.

Tot slot worden de beveiligingsadviezen gepubliceerd op de website van het NCSC. In voorkomende gevallen worden, conform de werkwijze met het TLP, bepaalde beveiligingsadviezen wel naar de deelnemende organisaties verzonden, maar niet gepubliceerd op de website.

3 Gebruik en waardering van de beveiligingsadviezen

3.1 Het gebruik van de beveiligingsadviezen in hoofdlijnen

Organisaties ontvangen beveiligingsadviezen op basis van hun foto
Zoals in hoofdstuk 3 geschetst, dienen partijen die zich aanmelden bij het NCSC aan de hand van een Exceloverzicht een 'foto' aan te leveren van de hard- en software die zij in gebruik hebben. Zo kan het NCSC de beveiligingsadviezen gericht versturen. Het is de verantwoordelijkheid van de organisatie zelf om wijzigingen tijdig aan het NCSC te melden.

Uit het onderzoek blijkt dat niet alle organisaties een (complete) foto hebben aangeleverd. Het gevolg is dat deze organisaties alle beveiligingsadviezen toegestuurd krijgen, waarvan een groot deel voor hen dus niet van toepassing is. Voor de organisaties die een grote ICT-afdeling hebben is het zelf filteren van de adviezen geen extra inspanning. Kleinere organisaties geven echter aan hier wel veel tijd en capaciteit aan kwijt te zijn.

Een aantal organisaties levert bewust een incomplete foto in om zo vooraf een selectie te maken van de adviezen die men van het NCSC wilt ontvangen. Zo laat men systemen bewust uit de foto omdat het binnen de eigen omgeving weinig risico's heeft. Een andere reden om bepaalde systemen uit de foto te houden, is dat men al voldoende betrouwbare adviezen van de betreffende leverancier van het systeem ontvangt.

Verder blijkt dat de organisaties die wel een foto hebben aangeleverd, niet altijd in staat zijn deze actueel te houden. Het gevolg hiervan is dat men geen adviezen ontvangt over kwetsbaarheden in soft- en hardware die recent in gebruik is genomen. Ook hier is weer het verschil te zien tussen de grotere organisaties en kleinere organisaties. Zo zijn er organisaties die elk kwartaal hun foto actualiseren en vervolgens aan het NCSC aanleveren.

Het inventariseren van de ICT-omgeving blijkt voor partijen vaak een omvangrijke (en ondoorzichtige) taak waar men lastig capaciteit voor kan organiseren. Men geeft aan dat men weet dat het eigenlijk wel moet, maar dat men er niet aan toekomt.

Daarnaast ervaren betrokkenen knelpunten in de wijze waarop de foto moet worden aangeleverd aan het NCSC. Niet alle aangesloten partijen ervaren het Exceloverzicht als goed werkbaar. Het is volgens hen een omvangrijk overzicht waarop alle mogelijke hard- en software opgesomd is, dat

in zijn geheel moet worden doorgenomen. Als een organisatie periodiek zijn foto wil updaten, dient het gehele Exceloverzicht iedere keer ingevuld te worden. Daarnaast bestaat de mogelijkheid dat een systeem dat in gebruik is bij een organisatie, niet op het overzicht staat.

Een aantal respondenten doet de aanbeveling om de foto digitaal te actualiseren, bijvoorbeeld door een besloten webportaal op de NCSC-website te maken voor aangesloten partijen. Zij kunnen dan naar hun eigen account gaan en daar hun foto bijwerken.

Loketfunctie per organisatie verschillend ingericht

Het NCSC verstuurt de beveiligingsadviezen per e-mail naar het adres dat de organisatie heeft opgegeven. Afhankelijk van hoe het intakeproces ('het loket') bij de betreffende organisatie is ingericht, komt het advies binnen in een centrale mailbox voor ICT/security-meldingen, of specifiek gericht aan (een aantal) functionarissen. Op deze adressen komen doorgaans ook de meldingen vanuit andere bronnen binnen. In geval van een high-high advies geven respondenten aan dat zij ook altijd meteen telefonisch worden geïnformeerd door het NCSC als zij in hun foto hadden aangegeven de betreffende software en/of systemen te gebruiken.

De organisaties met een grote security-afdeling houden de meldingen in de mailbox structureel in de gaten. Zo zijn er organisaties met een 24-uurs bezetting. Bij organisaties met minder capaciteit is de bewaking minder structureel en is het moment van verwerking van het advies afhankelijk van de frequentie waarmee de verantwoordelijke functionaris zijn e-mail bekijkt.

Alle beveiligingsadviezen worden gelezen en beoordeeld

Uit het onderzoek blijkt dat elke organisatie (in principe) alle beveiligingsadviezen leest en afweegt wat het betekent voor de eigen organisatie. De meeste organisaties verwerken de beveiligingsadviezen handmatig. Op hoofdlijnen worden daarbij de volgende vragen gesteld:

1. *Gebruikt de organisatie de software waar het advies over gaat?*

Zoals eerder gesteld heeft niet iedere organisatie een (actuele) foto van de ICT-omgeving aangeleverd waardoor zij alle adviezen binnenkrijgen en deze filtering noodzakelijk is. In het onderzoek geeft 90% van de ondervraagden aan dat dit de meest voorkomende reden is om een beveiligingsadvies niet op te volgen.

2. *Zo ja, hoe groot is de kans op uitbuiting?*

Hierbij kijkt men hoe toegankelijk het betreffende systeem is. Een applicatie die in verbinding staat met internet, is beter te bereiken en dus kwetsbaarder dan een applicatie die niet in verbinding staat met het internet. Vaak heeft men een breder pakket aan beveiligingsmaatregelen getroffen waardoor een lek in een specifiek systeem of applicatie niet direct een grote impact heeft.

3. *Welke gevolgen heeft uitbuiting voor de bedrijfsprocessen?*

Organisaties hanteren een eigen schaal waarmee kwetsbaarheden worden beoordeeld en gerangschikt naar prioriteiten. Het uitvallen van primaire systemen en het wegvallen van de dienstverlening krijgt hoge prioriteit, het tijdelijk niet beschikbaar zijn van een website heeft lagere prioriteit. Sommige organisaties hebben een uitgewerkt model van prioritering, bij andere organisaties is het een kwestie van 'professional judgement'.

4. Welke actie is op dit moment noodzakelijk: 'moet het nu of kan het wachten?'

Nadat een beveiligingsadvies op inhoud is beoordeeld, wordt bekeken wat dit voor de organisatie betekent. Organisaties maken een eigen risico-inschatting, die kan afwijken van de inschaling door het NCSC. Deze afwijking hoeft in de ogen van aangesloten organisaties niet ernstig te zijn, omdat het NCSC niet op de hoogte kan of hoeft te zijn van de volledige ICT-infrastructuur van aangesloten organisaties. De organisatie behoudt immers de eigen verantwoordelijkheid over de veiligheid van hun systemen.

Als de kans op uitbuiting van de kwetsbaarheid klein is, dan overweegt men om het later op te pakken. Als er direct actie nodig is, dan wordt het advies doorgezet naar de verantwoordelijke functionarissen. Grotere organisaties hebben hiervoor een 'incident respons team', in de kleinere organisaties gaan de functionarissen die de melding ontvangen zelf aan de slag.

Implementatie met inachtneming gevolgen voor bedrijfsprocessen

Als helder is wat de kwetsbaarheid is en welke acties noodzakelijk zijn, moet de oplossing door de organisatie geïmplementeerd worden. Doorgaans is de oplossing om updates en patches te installeren. De patches die de minste impact hebben op de bedrijfsprocessen worden in 'reguliere' patchrondes geïnstalleerd. Om de bedrijfsprocessen zo min mogelijk te belasten, kiezen organisaties ervoor om geautomatiseerd software-updates/patches op vaste tijdstippen (wekelijks of maandelijks na kantoortijd) te installeren. Een probleem dat respondenten hierbij kunnen ervaren is echter dat de te patchen software weleens onderdeel is van een groter software-pakket. Het patchen van dat ene onderdeel kan dan problemen opleveren voor het grotere geheel.

Om het risico op het verstoren van de bedrijfsprocessen te minimaliseren worden patches vóór de installatie eerst in een testomgeving uitgeprobeerd ('virtueel gepatched'). In de zogenaamde 'OTA-straat' (ontwikkel, test en acceptatie) wordt bekeken welk effect de patch heeft op het systeem als geheel.

- In de onderzoeksperiode heeft het NCSC 4578 beveiligingsadviezen uitgebracht. Daarvan waren 2438 updatemeldingen van een eerder uitgebracht advies.
- 55% van de bevraagde organisaties implementeert, in het geval van een 'high high' beveiligingsadvies, de aangereikte oplossing meestal. 23% doet dit altijd.
- Indien organisaties geen actie ondernemen naar aanleiding van een 'high high' beveiligingsadvies, geeft 90% aan dat de reden hiervan is dat het advies niet op de organisatie van toepassing is.
- 94% van de bevraagde organisaties verwerkt de beveiligingsadviezen handmatig.
- 74% van de bevraagde organisaties heeft zelf maatregelen getroffen om kwetsbaarheden in software te detecteren.

'Mocht een patch namelijk niet werken, dan ligt niet het hele systeem plat.'

Indien het installeren van een patch niet mogelijk of wenselijk is, dan nemen organisaties (tijdelijk) alternatieve maatregelen. Zo kan bijvoorbeeld de route van het dataverkeer aangepast worden zodat deze 'om het lek in het systeem stroomt'.

Afhankelijk van de wijze waarop een organisatie de ICT-afdeling heeft ingericht, kunnen de professionals zelfstandig besluiten om de benodigde maatregelen in te voeren. In sommige organisaties moet dit ter besluitvorming worden voorgelegd aan het management. Zeker wanneer de betreffende maatregelen impact hebben op het bedrijfsproces (systemen kunnen hinder ondervinden) of als er financiële gevolgen aan vast zitten, is dit het geval.

Geen rol NCSC bij het controleren op implementatie

Het NCSC ziet, zoals eerder gesteld, voor zichzelf geen rol om te controleren of organisaties beveiligingsadviezen opvolgen. Het is primair de verantwoordelijkheid van organisaties zelf om kwetsbaarheden te verhelpen. Een bepaalde verantwoordingsplicht zou volgens het NCSC de vertrouwensrelatie ook niet ten goede komen, waardoor organisaties mogelijkerwijs minder informatie delen. Een dergelijke controlerende rol veronderstelt voorts diepgaande informatie over de ICT-infrastructuur van organisaties. Het NCSC acht deze informatie gezien haar rol niet nodig om te ontvangen.

De opvatting dat het niet de taak is van het NCSC om organisaties te controleren op opvolging van het advies wordt gedeeld door de bevraagde organisaties. Het gaat immers om hun eigen bedrijfsproces. Zij dragen zelf de verantwoordelijkheid voor de veiligheid van hun systemen. Wel geven (met name) de publieke organisaties aan zich voor te kunnen stellen dat overheidsorganisaties wel meer verantwoording zouden moeten afleggen, hetzij aan de eigen sectorale toezichthouder, hetzij aan het NCSC. Het gaat volgens hen over de veiligheid van de rijksoverheid. In de NCSS2 wordt hierover het volgende gesteld:

'Bestaande (sectorale) toezichthouders zullen vervolgens eveneens daar waar dat nog niet het geval is hun rol moeten verbreden om ook cybersecurity te omvatten, waarbij overlap/dubbeling dient te worden voorkomen.'

Op 12 december 2013 heeft de minister van Veiligheid en Justitie de Tweede Kamer geïnformeerd over het versterken van het NCSC[6]. Deze versterking ziet op drie onderdelen, namelijk 1) het verstevigen van de wettelijke grondslag van de taken en bevoegdheden van de minister van Veiligheid en Justitie op het terrein van cyber security, 2) het nader invulling geven aan het waarborgen van vertrouwelijkheid en 3) het versterken van de adviserende rol van het NCSC. De adviserende rol van het NCSC is versterkt met de bevoegdheid van de minister van Veiligheid en Justitie om, indien het verhelpen van een kwetsbaarheid niet gebeurt maar het NCSC dit wel nodig acht, het betreffende ministerie hierover op de hoogte te stellen.

3.2 De waardering van de beveiligingsadviezen

3.2.1 Positieve punten

Waardering voor de kennis en expertise van het NCSC

Uit het onderzoek blijkt dat vrijwel alle organisaties de kennis en expertise van de medewerkers van het NCSC waarderen. Om die reden nemen zij ook de beveiligingsadviezen die deze medewerkers verstrekken serieus. Op verschillende niveaus hebben medewerkers van het NCSC en

6 Brief van de minister van Veiligheid en Justitie aan de Tweede Kamer; 12 december 2013, nummer 26 643.

aangesloten organisaties regelmatig (informeel) contact met elkaar. De bij het onderzoek betrokken organisaties geven aan dat, in geval van incidenten, zij direct hun contactpersonen bij het NCSC kunnen bereiken en dat zij altijd bereidwillig zijn om te helpen.

Wel merken respondenten de afgelopen jaren een verandering in de benaderbaarheid van de NCSC te zien. In hun beleving had het NCSC – vooral ten tijde van voorloper GOVCERT – een meer operationele en laagdrempelige positie. De afgelopen jaren merkt men een ontwikkeling naar een meer strategische en formele positie en worden de contacten stroever ervaren dan voorheen. Zo geven betrokkenen aan dat 'er een behoorlijke tijd overheen kan gaan' voordat zij antwoord krijgen op een vraag.

Het NCSC geeft aan dat dit knelpunt te kunnen voorstellen. Dit heeft te maken met de veranderende schaalgrootte. De afgelopen periode is het NCSC als organisatie flink gegroeid en is de nodige tijd geïnvesteerd om de interne organisatie neer te zetten. Dit zou de contacten en dienstverlening beïnvloed kunnen hebben. In het kader van wederhoor geeft het NCSC aan dat men heeft gestreefd naar meer formele relaties met organisaties. De informele contacten zouden volgens het NCSC daar naast moeten kunnen blijven bestaan. De 24/7 bereikbaarheid is hier volgens hen juist voor bedoeld.

Adviezen vanuit NCSC zijn objectief en gezaghebbend

De beveiligingsadviezen van het NCSC hebben volgens respondenten een gezaghebbende status. In een internationaal speelveld met (concurrerende) private en publieke partijen, is een objectieve en onafhankelijke autoriteit[7], die boven alle belangen staat, volgens hen belangrijk. Leveranciers van systemen hebben hun eigen (commerciële) belangen. Zij publiceren een kwetsbaarheid in principe pas als zij ook een oplossing hebben. Betrokkenen geven in dat kader aan dat men het zou waarderen als het NCSC vaker informatie over kwetsbaarheden deelt, juist als er nog geen oplossing openbaar beschikbaar is.

'Veel leveranciers wachten met communiceren totdat zij een patch gereed hebben. In theorie kunnen dagen, zo niet weken, zitten tussen het moment dat een leverancier een kwetsbaarheid heeft ontdekt en het moment dat er een oplossing is geleverd. Als we eerder op de hoogte worden gesteld, dan is het mogelijk om andere tijdelijke maatregelen te treffen.'

Betrokkenen geven daarbij aan dat zij de indruk hebben dat softwareleveranciers sinds de komst van het NCSC bewuster zijn van de noodzaak om over kwetsbaarheden te publiceren. Voorheen publiceerden alleen beveiligingsbedrijven informatie over kwetsbaarheden, nu doen ook softwarebedrijven die niet op beveiliging gericht zijn dit. Dit heeft volgens hen mede te maken met de dwingende ogen van een onafhankelijke autoriteit als het NCSC.

De gezaghebbende status van het beveiligingsadvies helpt volgens betrokkenen ook om het eigen management te overtuigen van het kiezen voor een oplossing. Vaak blijkt 'cyber' nog een weinig tastbaar verschijnsel. Het is voor het management, met weinig affiniteit met ICT, lastig een adequate afweging te maken. Dan helpt het als een autoriteit een objectief advies geeft.

[7] Hiermee wordt niet een autoriteit op basis van wettelijk gezag bedoeld, maar de autoriteit die op basis van kennis en expertise deze positie heeft bemachtigd.

Organisaties veronderstellen gebruik van vertrouwelijke bronnen
In het onderzoek geven betrokkenen aan dat een belangrijke meerwaarde van het beveiligingsadvies van het NCSC het feit is dat deze, volgens hen, gebaseerd zijn op bronnen die voor andere organisaties niet te benaderen zijn. Het gaat dan bijvoorbeeld om informatie die vanuit inlichtingendiensten of bij andere (internationale) CERT'S is opgedaan. Het beeld dat betrokkenen van de beveiligingsadviezen hebben is echter niet helemaal correct. Zoals in hoofdstuk 2 is beschreven, zijn de meeste beveiligingsadviezen gebaseerd op openbare bronnen.

NCSC verstrekt informatie via meerdere kanalen
Veel betrokkenen geven aan dat zij informatie over kwetsbaarheden vooral ook uit andere NCSC-bronnen halen. Het gaat hen uiteindelijk om de informatie, het maakt niet uit op welke wijze (welk product) zij deze informatie verkrijgen. Via verschillende platforms (ISAC's, NDN) die door het NCSC worden georganiseerd, alsmede de (informele) directe contacten met NCSC-medewerkers, heeft men vaak eerder de benodigde informatie om maatregelen te treffen. Men ziet het NCSC als een coördinerende partij, een informatiemakelaar, die met haar eigen expertise de kennis over kwetsbaarheden kan verrijken.

'Het NCSC is de linking pin in het geheel om organisaties bij elkaar te brengen en om – in een vertrouwd netwerk – informatie te delen.

3.2.2 Ruimte voor verbetering

Beveiligingsadviezen zijn vaak niet de eerste melding voor organisaties
De meeste respondenten geven aan dat zij vaak al op de hoogte zijn van een kwetsbaarheid voordat zij een beveiligingsadvies van het NCSC ontvangen. Dit, omdat betrokkenen van dezelfde bronnen gebruik maken. De helft van de ondervraagden geeft aan de kwetsbaarheid te hebben verholpen voordat zij een advies had ontvangen. Men heeft hier over het algemeen ook wel begrip voor. Betrokkenen weten dat het NCSC de berichtgeving eerst analyseert en verifieert, voordat een advies openbaar wordt gemaakt. Het advies heeft voor hen dan vooral de functie van bevestiging en een checklist. Respondenten geven aan dat het echter ook wel voorkomt dat de tijd tussen bekend worden van een kwetsbaarheid en het publiceren van een advies te lang is – in sommige gevallen gaat het volgens hen om dagen. In dat kader geeft men aan dat het wenselijk is om eerder op de hoogte gebracht te worden van een mogelijke dreiging.

'Soms is 80% zekerheid ook voldoende om een inschatting te maken. Het risico dat er uiteindelijk geen kwetsbaarheid is en er voor niets werk is verricht, is te aanvaarden.'

Met name de organisaties met een grotere ICT-afdeling zijn vaak door het eigen netwerk al in vroegtijdig stadium op de hoogte gebracht van een kwetsbaarheid. Mede hierdoor is de informatie die het NCSC deelt, vaak dubbel met andere informatie en vindt er volgens hen nauwelijks verrijking door het NCSC plaats.

'Het uiteindelijke beveiligingsadvies ligt vaak voor de hand en komt als mosterd na de maaltijd.'

Het knelpunt dat deze partijen hierbij ervaren is dat zij wel steeds handmatig de adviezen moeten vergelijken met informatie die zij al in het bezit hebben. Voor deze partijen zou een beveiligingsadvies meerwaarde hebben als het zich (uitsluitend) zou richten op aspecten waar men geen

informatie over kan hebben. Een voorbeeld is informatie – vanuit het inlichtingennetwerk – over specifieke dreigingen voor Nederland en de betreffende organisatie in het bijzonder. De bulk van de – vooral minder urgente – beveiligingsadviezen kan volgens hen achterwege worden gelaten.

Andere partijen hechten er echter juist waarde aan om toch deze adviezen met een lagere kwalificatie te ontvangen. Enerzijds omdat ze zelf niet de capaciteit heeft om deze te achterhalen, anderzijds omdat zij van mening zijn dat een combinatie van deze kwetsbaarheden uiteindelijk een grote kwetsbaarheid kan vormen.

'Je hebt alle informatie nodig om zelf de afweging te kunnen maken of iets een kwetsbaarheid is voor je organisatie. Twee of meer 'medium' kwetsbaarheden samen kunnen tot een high-high leiden.'

Groot aantal updates van hetzelfde advies

Respondenten geven aan dat het NCSC een groot aantal adviezen uitbrengt, maar dat een groot deel daarvan een update van een eerdere beveiligingsadvies is. In de onderzoeksperiode heeft het NCSC 4578 beveiligingsadviezen gepubliceerd, waarvan 2438 updatemeldingen. Ruim de helft van alle uitgebrachte adviezen betrof dus een melding van een update van het advies. Inhoudelijk verandert er volgens betrokken niet veel aan het advies. Een update bevat vaak alleen een melding dat er nieuwe versies van de oplossing (patch) beschikbaar zijn op de website waar in het eerste advies al naar was verwezen.

Respondenten geven aan dat zij, na alerting van het eerste advies, vanzelf de bronwebsite in de gaten houden. Updatemeldingen zijn in die zin inhoudelijk overbodig. Maar het kost volgens hen iedere keer wel tijd om handmatig het advies langs te lopen om er zeker van de zijn dat er geen nieuwe belangrijke informatie in staat.

Slordigheidsfoutjes in de beveiligingsadviezen

In het onderzoek geven respondenten aan dat beveiligingsadviezen weleens fouten bevatten. Oplossingen in een beveiligingsadvies worden doorgaans geknipt en geplakt uit de primaire bron waar het NCSC de kwetsbaarheid heeft gevonden. Het kan dan voorkomen dat er weleens dubbele spaties of een foutief adres van een website in het advies terechtkomen. Het gevolg hiervan is dat organisaties de verbeteringen niet geautomatiseerd kunnen doorvoeren.

Het NCSC geeft in het onderzoek aan dit knelpunt te herkennen. Door de groei van de waakdienst en het inwerken van nieuw personeel is de kwaliteit van het product teruggelopen. De schaalvergroting was volgens het NCSC nodig om de toegenomen hoeveelheid werk te kunnen verrichten, maar heeft dit als neveneffect gehad. De verwachting bij het NCSC is dat het om een tijdelijke dip in de kwaliteit gaat.

Verschillende abstractieniveaus van de beveiligingsadviezen gewenst

De bij dit onderzoek betrokken organisaties hebben een zeer divers beeld over de inhoud van de beveiligingsadviezen. Een groep vindt de beveiligingsadviezen te technisch en heeft vooral behoefte aan 'kwalitatieve' informatie in het advies. Zo zouden deze respondenten bijvoorbeeld meer contextinformatie willen hebben over methodes en technieken die gebruikt worden, een motief of een link naar specifieke actoren of andere dreigingen. Ook een meer uitgebreide duiding van de impact van de kwetsbaarheid zou volgens hen wenselijk zijn, omdat hiermee leidinggevenden – met minder inhoudelijke kennis van ICT – beter geïnformeerd kunnen worden.

Hiertegenover staat de groep die de adviezen te algemeen vindt. Deze respondenten hebben behoefte aan een meer technische duiding. Zij beschouwen het advies vooral als alertering en zoeken zelf in de bron naar oplossingen. Zo geeft 91% van de bevraagde organisaties aan dat het aanvullen van de beveiligingsadviezen met informatie over detectiemethoden wenselijk is. Hierbij valt te denken aan 'indicators of compromise', waarmee een organisatie kan controleren of er daadwerkelijk misbruik is gemaakt van de kwetsbaarheid en of deze schade heeft opgeleverd.

Conclusie

Uit het onderzoek blijkt dat de aangesloten organisaties het belang van cybersecurity onderschrijven en dit opvatten als een eigen verantwoordelijkheid. Ten behoeve hiervan proberen organisaties zo veel mogelijk (geverifieerde) informatie over kwetsbaarheden binnen te halen. De beveiligingsadviezen van het NCSC zijn hiervoor een van de bronnen dan wel de voornaamste bron.

De Inspectie heeft geconstateerd dat alle partijen elk beveiligingsadvies bekijken, wegen en – naar eigen inzicht – de noodzakelijke maatregelen treffen. Het beveiligingsadvies blijkt hierin een belangrijke, maar niet onmisbare bron. Het overgrote deel van de beveiligingsadviezen bevat namelijk informatie die men vanuit andere bronnen - vaak eerder en uitgebreider – heeft gekregen. Het beveiligingsadvies van het NCSC heeft daarmee meer het karakter van een alertering en een bevestiging. De meerwaarde is eerder te vinden in de positie van het NCSC als onafhankelijke kennisautoriteit dan in het product zelf. Uiteindelijk gaat het de betrokken organisaties niet om 'het product beveiligingsadviezen', maar om de informatie vanuit het NCSC die hen, op welke wijze dan ook, bereikt.

4 Conclusie

De Inspectie VenJ heeft onderzocht wat aangesloten organisaties doen met de beveiligingsadviezen van het NCSC en wat de meerwaarde er van is voor de ontvangende partijen. Uit het onderzoek blijkt dat alle organisaties de beveiligingsadviezen van het NCSC lezen, beoordelen en indien nodig de noodzakelijke maatregelen treffen. Zij bezien hierbij of de betreffende software in gebruik is, hoe groot de kans op uitbuiting is gegeven organisatie specifieke factoren, welke gevolgen uitbuiting heeft voor de bedrijfsprocessen en hoe dringend actie nodig is.

De meeste organisaties beschouwen de beveiligingsadviezen – in de huidige vorm – als 'bruikbaar, maar niet onmisbaar'. Vaak heeft men informatie over kwetsbaarheden al via andere bronnen (zowel externe als andere informatiekanalen van het NCSC) binnengekregen en de oplossing geïmplementeerd, voordat het beveiligingsadvies is ontvangen. Voor alle partijen zit de meerwaarde van de beveiligingsadviezen niet zo zeer in de inhoud en kwaliteit, maar voornamelijk in het feit dat de adviezen afkomstig zijn van een onafhankelijke autoriteit met een gezaghebbende positie. Het NCSC kan volgens hen over de – commerciële – schotten kijken en een objectief advies leveren. Opvallend daarbij is de veronderstelling van aangesloten organisaties dat het NCSC de beveiligingsadviezen (ook) baseert op vertrouwelijke informatiebronnen waar de organisaties zelf geen toegang tot hebben. Want hoewel de aangesloten organisaties dit als belangrijke meerwaarde zien, baseert het NCSC beveiligingsadviezen in beginsel op openbare bronnen.

De Inspectie concludeert dat de beveiligingsadviezen in de huidige vorm beperkte meerwaarde hebben. De Inspectie onderschrijft de ambitie van het NCSC om haar capaciteiten zo efficiënt en effectief mogelijk in te zetten. In dat kader beveelt de Inspectie het NCSC aan om het product beveiligingsadviezen te heroverwegen. Het gaat de aangesloten organisaties uiteindelijk om de informatie over kwetsbaarheden, niet om het product of de wijze waarop ze de informatie binnen krijgen. De Inspectie gaat er vanuit dat de in dit onderzoek geconstateerde aandachtspunten hierbij worden betrokken. (zie voor een volledig overzicht bijlage I).

Verbeterpunten

- Het actief vragen aan partijen om een (actuele) foto aan te leveren zodat zij geen overbodige adviezen meer ontvangen.
- Het vereenvoudigen van de wijze waarop organisaties een ‘foto’ van de eigen ICT-omgeving aanleveren en actualiseren, bijvoorbeeld door een besloten webportaal in te richten waar organisaties dit digitaal kunnen doen.
- Het verbeteren van de bereikbaarheid van het NCSC zodat men sneller op vragen van aangesloten organisaties kan reageren.
- Het indikken van de productie zodat aangesloten partijen alleen adviezen krijgen die echt belangrijk zijn. Dit kan door:
  - alleen hoger gekwalificeerde kwetsbaarheden (medium/high) uit te brengen;
  - geen updatemeldingen meer te doen;
  - niet meer de standaardadviezen te leveren die men normaal gesproken van grote leveranciers zelf al krijgt.
- Het inhoudelijk verrijken van het advies en dit meer toe te schrijven naar de verschillende doelgroepen aan wie het advies is gericht. Voor de experts betekent dit meer gedetailleerde technische informatie in het advies opnemen. Voor het management betekent dit meer contextinformatie over de mogelijke gevolgen van de kwetsbaarheid en de te implementeren oplossing.
- Het eerder uitbrengen van informatie over mogelijke kwetsbaarheden – nog voordat er een oplossing beschikbaar is – zodat organisaties eerder (alternatieve) maatregelen kunnen treffen.
- Het concentreren op adviezen die niet gebaseerd zijn op (openbare) bronnen waar partijen zelf toegang tot (kunnen) hebben.
- Het concentreren op adviezen die gericht zijn op specifieke dreigingen voor Nederland, een sector of een individuele organisatie.

II Voorbeeld 'high high' beveiligingsadvies

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

   #####################################################
  ##   N C S C ~ B E V E I L I G I N G S A D V I E S   ##
 #####################################################

######################## UPDATE 1.02
#############################

Titel              : Diverse kwetsbaarheden in OpenSSL verholpen
Advisory ID        : NCSC-2015-0208
Versie             : 1.02
Kans               : high
CVE ID             : CVE-2015-0204, CVE-2015-0207, CVE-2015-0208,
                     CVE-2015-0209, CVE-2015-0285, CVE-2015-0286,
                     CVE-2015-0287, CVE-2015-0288, CVE-2015-0289,
                     CVE-2015-0290, CVE-2015-0291, CVE-2015-0292,
                     CVE-2015-0293, CVE-2015-1787
                     (http://cve.mitre.org/cve/)
Schade             : high
                     Denial-of-Service (DoS)
                     Omzeilen van beveiligingsmaatregel
                     Toegang tot gevoelige gegevens
Uitgiftedatum      : 20150320
Toepassing         : OpenSSL OpenSSL
                     OpenSSL Project OpenSSL
Versie(s)          :
Platform(s)        : Ubuntu
                     Debian
                     FreeBSD
                     SUSE
                     OpenBSD

Update
   SUSE, Ubuntu, FreeBSD en OpenBSD hebben updates vrijgegeven
om de
   kwetsbaarheden in OpenSSL te verhelpen.

Samenvatting
   De ontwikkelaars van OpenSSL hebben updates vrijgegeven die
een
   aantal kwetsbaarheden verhelpen waarmee onder andere mogelijk
   gevoelige gegevens verkregen kunnen worden of een Denial-of-
Service
   veroorzaakt kan worden.

Gevolgen
   Een kwaadwillende kan makkelijker data bemachtigen uit
   OpenSSL-sessies of applicaties/servers/clients die OpenSSL
   gebruiken laten crashen.

Beschrijving
```

```
   - CVE-2015-0204:
   Deze kwetsbaarheid bevindt zich in OpenSSL versies 1.0.1,
1.0.0 en
   0.9.8 en is eerder omschreven in NCSC advisory NCSC-2015-
0013.

   De OpenSSL client accepteert het gebruik van een tijdelijke
RSA key
   binnen een non-export RSA key exchange ciphersuite. Een
   kwaadwillende kan de kwetsbaarheid misbruiken door een server
een
   zwakke tijdelijke RSA key te laten aanbieden, om daarmee de
   versleutelde verbinding minder veilig te maken.

   Deze kwetsbaarheid is eerder verholpen door OpenSSL, maar nu
   opnieuw door hen ingeschaald. De inschaling is van low naar
high
   gegaan omdat OpenSSL het gebruik van RSA export ciphersuites
   verkeerd in heeft geschat.

   - CVE-2015-0207:
   Deze kwetsbaarheid bevindt zich in OpenSSL versie 1.0.2.

   De DTLS-feature in OpenSSL bevat in de DTLSv1_listen functie
een
   kwetsbaarheid. Deze kwetsbaarheid wordt veroorzaakt doordat
deze
   functie data van vorige aanroepen in het interne SSL-object
   bewaart.
   Hierdoor kunnen segfaults optreden, bijvoorbeelt door een
   ClientHello-bericht. Dit leidt dan tot een Denial-of-Service
(DoS).

   - CVE-2015-0208:
   OpenSSL-versie 1.0.2 is kwetsbaar voor deze kwetsbaarheid.

   Deze kwetsbaarheid betreft een fout in de code voor
   certificaat-controles, waardoor een aanvaller deze
kwetsbaarheid
   uit kan buiten door een certificaat aan te bieden dat
gecontroleerd
   wordt.
   Alle toepassingen, zowel clientside als serverside, die
OpenSSL
   gebruiken voor clientcertificaatverificatie zijn in potentie
   kwetsbaar voor deze Denial-of-Service (DoS) aanval.

   - CVE-2015-0209:
   Deze kwetsbaarheid bevindt zich in OpenSSL versies: 1.0.2,
1.0.1,
   1.0.0 en 0.9.8.

   Als een malafide EC private key file wordt gebruikt via de
   d2i_ECPrivateKey functie, kan dit tot een use after free
probleem
   leiden. Hierdoor kan een DoS-aanval of geheugencorruptie
   plaatsvinden. Hiervoor moet de applicatie echter wel
onvertrouwde
```

```
   EC private keys accepteren.

   - CVE-2015-0285:
   OpenSSL-versie 1.0.2 is in client mode kwetsbaar voor deze
   kwetsbaarheid.

   De client kan een handshake doen met een unseeded PRNG
(pseudo
   random number generator). Hierdoor kan de output van de
handshake
   voorspelbaar worden en daardoor minder vertrouwelijk.

   Dit is te controleren op een potentieel kwetsbare machine
door
   "openssl s_client -psk 1a2b3c4d -tls1_2 -cipher PSK-RC4-SHA"
uit te
   voeren. Als dit commando slaagt is de machine kwetsbaar voor
deze
   kwetsbaarheid.

   - CVE-2015-0286:
   OpenSSL-versies 1.0.2, 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar
voor
   deze kwetsbaarheid.

   De functie  ASN1_TYPE_cmp zal crashen als deze ASN.1 boolse
types
   in ASN-documenten verwerkt. Deze functie wordt gebruikt bij
   bepaalde certificaat-controles, waardoor een aanvaller deze
   kwetsbaarheid uit kan buiten door een certificaat aan te
bieden dat
   gecontroleerd wordt.

   Alle toepassingen, zowel clientside als serversize, die
OpenSSL
   gebruiken voor clientcertificaatverificatie zijn in potentie
   kwetsbaar voor deze Denial-of-Service (DoS) aanval.

   - CVE-2015-0287:
   OpenSSL-versies 1.0.2, 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar
voor
   deze kwetsbaarheid.

   Een fout in het hergebruik van geheugen in de  ASN1-parser
kan een
   aanvaller in staat stellen geheugencorruptie te laten
plaatsvinden.
   De makers van OpenSSL raden dit hergebruik dan ook af.
Applicatie
   die ASN1 berichten parsen met CHOICE of ANY DEFINED BY
componenten
   zijn kwetsbaar, maar niet in het geval van het parsen van
   certificaten. Normaliter leidt geheugencorruptie tot crashes
van de
   applicatie in kwestie.


   - CVE-2015-0288:
```

```
   OpenSSL-versies 1.0.2, 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar
voor
   deze kwetsbaarheid.

   In de X509_to_X509_REQ functie bevindt zich een NULL pointer
   dereference kwetsbaarheid, als de certificaat keyfile
ongeldig is.


   - CVE-2015-0289:
   OpenSSL-versies 1.0.2, 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar
voor
   deze kwetsbaarheid.

   Applicaties die  PKCS#7 signatures controleren, of anderszins
met
   onvertroude PKCS#7 data omgaan kunnen kwetsbaar zijn voor
deze
   kwetsbaarheid. OpenSSL clients en server zelf zijn niet
kwetsbaar.

   - CVE-2015-0290:
   Deze ernstige kwetsbaarheid treft alleen versie 1.0.2.

   Alleen x86_64 platforms die AES NI instructies ondersteunen
zijn
   kwetsbaar. Een pointer-kwetsbaarheid in de multiblock feature
in
   OpenSSL kan leiden tot een Denial-of-Service (DoS).

   - CVE-2015-0291:
   Deze ernstige kwetsbaarheid treft alleen versie 1.0.2.

   Als een client een renegotiation uitvoert in een SSL
verbinding kan
   een null pointer dereference optreden. Hierdoor kan een
   Denial-of-Service (DoS) ontstaan.

   - CVE-2015-0292:
   OpenSSL-versies 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar voor
deze
   kwetsbaarheid.

   In OpenSSL bevindt zich een kwetsbaarheid in de verwerking
van
   base64-gecodeerde data. Alle code die OpenSSL gebruikt om
base64
   data te interpreteren kan kwetsbaar zijn, zoals bijvoorbeeld
   PEM-verwerkende code. Een malafide base64-bericht kan een
segfault
   of geheugencorruptie veroorzaken. Deze kwetsbaarheid is
verholpen
   in diverse nieuwe OpenSSL versies, maar nog niet als patch
voor
   oudere versies aangeboden.

   - CVE-2015-0293:
```

```
   OpenSSL-versies 1.0.2, 1.0.1, 1.0.0 en 0.9.8 zijn kwetsbaar
voor
   deze kwetsbaarheid.

   Een kwaadwillende kan een OPENSSL_assert veroorzaken in
servers die
   zowel SSLv2 als export cipher suites ondersteunen. Hiervoor
dient
   de client een malafide SSLv2 bericht te sturen met een
   CLIENT-MASTER-KEY inhoud.

   - CVE-2015-1787:
   Deze ernstige kwetsbaarheid treft alleen versie 1.0.2.

   Als de OpenSSL-machine client authenticatie doet kan een
segfault
   optreden als een DHE ciphersuite wordt gebruikt. en een
   ClientKeyExchange wordt verstuurd door de client met een
lengte 0.
   Dit kan leiden tot een Denial-of-Service (DoS).

Mogelijke oplossingen
   De ontwikkelaars van OpenSSL hebben updates beschikbaar
gemaakt om
   de kwetsbaarheden te verhelpen. De volgende updates zijn
   beschikbaar:

   Versies 1.0.2*: verholpen in versie 1.0.2a.
   Versies 1.0.1*: verholpen in versie 1.0.1m.
   Versies 1.0.0*: verholpen in versie 1.0.0r.
   Versies 0.9.8*: verholpen in versie 0.9.8zf.

   De nieuwste versies van de OpenSSL zijn beschikbaar via:
   http://openssl.org/source/

   -= Debian =-
   Debian heeft updates van openssl beschikbaar gesteld voor
Debian
   7.0 (Wheezy) om de kwetsbaarheden te verhelpen. U kunt de
   aangepaste packages installeren door gebruik te maken van
'apt-get
   update' en 'apt-get upgrade'. Meer informatie kunt u vinden
op
   onderstaande pagina:

   https://lists.debian.org/debian-security-announce/2015
      /msg00082.html

   -= FreeBSD =-
   FreeBSD heeft updates beschikbaar gesteld om de
kwetsbaarheden te
   verhelpen in . U kunt deze updates installeren via freebsd-
update.
   Meer informatie over deze updates vindt u op:

   http://vuxml.freebsd.org/freebsd
      /9d15355b-ce7c-11e4-9db0-d050992ecde8.html
```

```
   -= OpenBSD =-

   OpenBSD heeft updates beschikbaar gesteld om de kwetsbaarheid
te
   verhelpen. U kunt deze updates installeren via pkg-add. Meer
   informatie over deze updates vindt u op:

   http://www.openbsd.org/errata55.html

   -= SUSE =-
   SUSE heeft updates beschikbaar gesteld om de kwetsbaarheden
te
   verhelpen in SUSE 12. U kunt deze aangepaste packages
installeren
   door gebruik te maken van 'YaST'. U kunt het package ook
handmatig
   downloaden van de SUSE FTP-server (ftp.suse.com). Voor meer
   informatie, zie:

   http://lists.opensuse.org/opensuse-security-announce/2015-03
      /msg00022.html

   -= Ubuntu =-
   Ubuntu heeft updates beschikbaar gesteld voor Ubuntu 10.04
LTS,
   12.04 LTS, 14.04 LTS, 14.10 om de kwetsbaarheden te
verhelpen. U
   kunt de aangepaste packages installeren door gebruik te maken
van
   'apt-get update' en 'apt-get upgrade'. Meer informatie kunt u
   vinden op onderstaande pagina:

   http://www.ubuntu.com/usn/usn-2537-1/

Hyperlinks
   http://openssl.org/news/secadv_20150319.txt
   http://openssl.org/source/

Vrijwaringsverklaring
   Door gebruik van deze security advisory gaat u akkoord met de
   navolgende voorwaarden. Ondanks dat het NCSC de grootst
mogelijke
   zorg heeft betracht bij de samenstelling van dit
beveiligingsadvies,
   kan het NCSC niet instaan voor de volledigheid, juistheid of
   (voortdurende) actualiteit van dit beveiligingsadvies. De
informatie
   in dit beveiligingsadvies is uitsluitend bedoeld als algemene
   informatie voor professionele partijen. Aan de informatie in
dit
   beveiligingsadvies kunnen geen rechten worden ontleend. Het
NCSC
   en de Staat zijn niet aansprakelijk voor enige schade ten
gevolge
   van het gebruik of de onmogelijkheid van het gebruik van dit
   beveiligingsadvies, waaronder begrepen schade ten gevolge van
de
   onjuistheid of onvolledigheid van de informatie in dit
```

```
   beveiligingsadvies. Op dit beveiligingsadvies is Nederlands
recht
   van toepassing. Alle geschillen in verband met en/of
voortvloeiend
   uit dit beveiligingsadvies zullen worden voorgelegd aan de
exclusief
   bevoegde rechter te Den Haag. Deze rechtskeuze geldt tevens
voor de
   voorzieningenrechter in kort geding.
```

-----BEGIN PGP SIGNATURE-----
Version: Encryption Desktop 10.3.2 (Build 15495)
Charset: utf-8

wsDVAwUBVQwMIJsHXCBfNcE4AQgwmgv8C1rqDCYkhJOUrCAUxwP/k/rlSAjjJ3ND
lnQMzQfWcKtlMQ64BfSslJuWn9+GqmBuILPO7PICWHnp27gKfgBAMeL0k93WF/H6
wmTweNn5CkFyytRA6hxy3tYTYNIxIJV6HNk4hKHcEmwpp1EsZ7T38FZYHqYuD/IU
K235AwRbmNFKQloAg55JSqci7yA/0b/UlaiF2GQGK+I3f3B/WyW2qApYmuf+wjur
AQn+v+SMlhE63kUGaWvwPQ7ynyjGYx4Bgeqmd/ibNX00VWyd9GQ6Sx3WCDYHrn4T
4DwaDyyxTokzPWvQQB1QViybd0Dc9BCd+9FGT6mmVGieTAdxMHZYjSsJnpk97tt8
3y1id3G6S5Vn4Xzkxin+ChrBZk9aZcQVfNuKcMEia8eyXNlTz5xVtFxsW2yfUPNk
8DsCwUXUdVyebJJQ8Klhe3BUrUbw4LTlr1cv+DCGeDqWnU47Rxek4bvcuI1+Xd16
lLEmHi8MiTrV400pWVhpyhjTMBLqykbM
=lb0s
-----END PGP SIGNATURE----

III Documentatie

- Brief van de minister van Veiligheid en Justitie aan de Tweede Kamer; 12 december 2013, nummer 26 643
- Cybersecuritybeeld Nederland 2014
- Factsheet missie DCS-NCSC
- Factsheet Nationaal Detectie Netwerk
- Folder NCSC; 'Het Nationaal Cyber Security Centrum biedt slagkracht door samenwerking'
- Inschalingsmatrix beveiligingsadviezen
- NCSC producten- en dienstenoverzicht
- Nationale Cyber Security Strategie 2
- Overzicht uitgebrachte beveiligingsadviezen periode 1 januari 2012 – 1 september 2014

IV Afkortingen

CERT	Computer Emergency Response Team
CVE	Common Vulnerabilities and Exposures
ICT	Informatie- en Communicatie Technologie
ISAC	Information Sharing and Analysis Center
NCSC	Nationaal Cyber Security Centrum
NCSS(2)	Nationale Cyber Security Strategie (2)
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
TLP	Traffic Light Protocol
XML	Extensible Markup Language

Missie Inspectie Veiligheid en Justitie

De Inspectie Veiligheid en Justitie houdt voor de samenleving, de ondertoezichtgestelden en de politiek en bestuurlijk verantwoordelijken toezicht op het terrein van veiligheid en justitie om inzicht te geven in de kwaliteit van de taakuitvoering en de naleving van regels en normen, om risico's te signaleren en om organisaties aan te zetten tot verbetering. Hiermee draagt de Inspectie bij aan een veilige en rechtvaardige samenleving.

Dit is een uitgave van:
Inspectie Veiligheid en Justitie
Ministerie van Veiligheid en Justitie
Turfmarkt 147 | 2511 DP Den Haag
Postbus 20301 | 2500 EH Den Haag
communicatie@inspectievenj.nl | www.ivenj.nl

Mei 2015 | Publicatienummer: 86097